From:	ehud barak <ehbarak1@gmail.com>
To:	Gary Fegel <gary@fegel.com>
CC:	Pavel Gurvich <pavel@guardicore.com>
Date:	Thu, 1/9/2014 7:52:44 PM
Subject:	Re: (BV) Real-Life Hazards Await as ¡®Internet of Things¡¯ Catches On: View

Hi All
True. I propose we sit down with Pavel. And possibly another one or two people Pavel recommends or otherwise agreed upon in advance, for a brainstorming on future directions and actions that are preconditions for success in this newly emerging field. It includes needed insights not just on technology but several other social psychological and market related aspects.
The earlier the better.
Best
EB

Sent from my iPhone

> On Jan 9, 2014, at 15:12, Gary Fegel wrote:
>
> Pavel
>
> I think you were perfectly right in what you mentioned to Ehud and myself in London: Forget mobile phone security, that¡¯s a crowded place. The next big thing is in all the small devices. I have learned the name: Apparently it¡¯s called ¡°the internet of things¡±. Interestingly enough I suddenly read about it everywhere. Below is a short article I picked up on Bloomberg today which sais it all. Of course we aren¡¯t the first ones, but it¡¯s clear that the security aspect in this field is a lot less advanced yet. This is what we need to do !!
>
> See you next week.
> Gary
>
>
>>
>> Real-Life Hazards Await as ¡®Internet of Things¡¯ Catches On: View
>> 2014-01-08 23:17:33.146 GMT
>>
>>
>> By the Editors
>> Jan. 8 (Bloomberg) -- At the International Consumer
>> Electronics Show in Las Vegas, an annual carnival of corporate
>> hype and techno-hoopla, John Chambers, the head honcho at Cisco
>> Systems Inc., described an emerging phenomenon in terms that
>> were sensationalist even by Vegas standards.
>> ¡°It will be bigger than anything that¡¯s ever been done in
>> high tech,¡± he said. ¡°It will change the way people live, work
>> and play.¡± And, oh yes, it¡¯s a $19 trillion opportunity.
>> The phenomenon is commonly known as the Internet of Things.
>> As more and more objects -- appliances and automobiles, tennis
>> rackets and toothbrushes -- are wired with sensors and connected
>> to the Internet and to other devices, they¡¯re pulsing with new
>> information and capabilities. Cisco has estimated that 25
>> billion devices will be connected to the Internet by next year,

>> and 50 billion by 2020.
>> The potential benefits of this evolution are compelling.
>> Yet as with every innovation of the digital era, it¡¯s also
>> fraught with perils -- many of which we haven¡¯t even begun to
>> think through.
>> Enthusiasts argue that connecting more and more objects
>> will help bring the automation and precision of the digital
>> world to bear on the inconveniences of the physical one.
>> Consumers -- who can already buy communicative door locks, pet
>> collars, forks, fitness monitors, light bulbs, inhalers,
>> thermostats and so on -- might one day see their domestic
>> routines unfold with Jetsons-like ease.
>> Retailers could use ¡°smart¡± sensors to better organize
>> their inventory and track performance data. Manufacturers could
>> improve logistics, reduce waste and boost productivity. And city
>> governments might benefit from smart roads that monitor
>> congestion, trash cans that tell garbagemen when they¡¯re full or
>> parking meters that ping drivers when a spot opens up.
>> What could possibly go wrong?
>> For starters, like any new technology, such devices will be
>> prone to malfunctions, which can be pretty alarming when it
>> comes to your home appliances or your car. It¡¯s also unclear how
>> much this evolution is being driven by real demand -- have you
>> ever thought to yourself: ¡°This toothbrush is awesome, I just
>> wish it could communicate with my smartphone"? -- and how much
>> by the relentless hype cycle of the technology business. Many
>> devices now use smart technology whether you like it or not.
>> More alarming are the twinned perils of the networked age:
>> security and privacy. The Internet of Things could extend both
>> dangers from the virtual world into the physical one in new and
>> unpredictable ways.
>> Many connected devices are manufactured by companies that
>> have no experience in warding off online intrusions, and
>> consumers often don¡¯t bother to download security patches. The
>> results are predictable. Hackers have easily exploited
>> electronic security systems in cars, used a flaw in electronic
>> locks to break into dozens of hotels rooms and compromised all
>> manner of home appliances. One deviant hacked a baby monitor and
>> said disgusting things to a 2-year-old. Researchers have warned
>> about vulnerabilities in home routers, medical devices and
>> industrial systems. You probably don¡¯t want to think about the
>> implications of an attack on a smart toilet.
>> To say that worse intrusions are inevitable isn¡¯t to be
>> alarmist; it¡¯s to acknowledge that cybersecurity is a deeply
>> imperfect science that¡¯s about to face a lot of new challenges.
>> Protecting privacy will also get harder -- and the
>> government isn¡¯t the only snooper to worry about. When companies
>> want to collect data about everything you do in exchange for an
>> app or service, chances are their motives aren¡¯t entirely
>> altruistic. A good tipoff to their true intentions is that
>> advertisers are licking their chops at CES this year. When
>> everything from your front door to the car you drive to the
>> shops you visit collects and stores data about you, your ability
>> to control any of it -- let alone escape from relentless

>> marketing -- looks harder and harder.
>> So what to do?
>> Market-based solutions to these problems would be welcome,
>> but in practice they¡¯ve proved elusive. It¡¯s hard to be a
>> rational consumer, for instance, when so much data is being
>> collected about you surreptitiously, often explained (if at all)
>> in small-print legalese. Mozilla, the nonprofit behind the
>> Firefox Internet browser, is onto something in this regard with
>> an add-on called Lightbeam, which shows users who¡¯s tracking
>> them as they move from site to site. Such technology will need
>> to get a lot more sophisticated, and a lot more widely adopted,
>> before it spurs companies to take privacy seriously as the
>> Internet of Things expands.
>> In the meantime, hardware engineers should get used to
>> incorporating better security into their designs. Manufacturers
>> should be far more vigilant about online threats to their
>> products. The government should require companies to be more
>> transparent about what data they collect. And the poor,
>> bewildered consumer should heed one other thing John Chambers
>> said. The Internet of Things, he told the crowd, ¡®¡®changes
>> people¡¯s lives forever.¡±
>>
>> For Related News and Information:
>> For more Bloomberg View: VIEW
>>
>> --Editors: Timothy Lavin, Clive Crook.
>>
>> Click on ¡°Send Comment¡± in sidebar display to send a letter to
>> the editor.
>>
>> To contact the Bloomberg View editorial board:
>> view@bloomberg.net.
>